DEC STD 205-2 Product Fault Management Specification: Hardware Life Cycle Guidelines

DOCUMENT IDENTIFIER: A-DS-EL00205-02-0000 Rev A, 10-Jul-1992

ABSTRACT: This section provides detailed life cycle guidelines for developing a hardware product fault management specification.

APPLICABILITY: This section provides guidance for anyone writing a hardware Product Fault Management Specification.

STATUS: APPROVED 10-Jul-1992; use VTX SMC for current status.

This document is confidential and proprietary, and is the property of Digital Equipment Corporation. It is an unpublished work protected under applicable copyright laws.

© Digital Equipment Corporation. 1992. All rights reserved.

DEC STD 205-2 Product Fault Management Specification: Hardware Life Cycle Guidelines

DOCUMENT IDENTIFIER: A-DS-EL00205-02-0000 Rev A, 10-Jul-1992

REVISION HISTORY:	No previous revision exists.
Document Management Category:	Digital Services Requirements (FR)
Responsible Department:	Digital Services Engineering
Responsible Person:	Mike Robey
SMC Writer:	Ellie DeVries

APPROVAL: This document has been reviewed and recommended for approval by the General Review group for its category.

Mike Robey - Digital Services Engineering

Eric Williams - Standards Process Manager

Direct requests for further information to:

Mike Robey
Use $ VTX ELF for the latest location information.

Use VTX SMC to order copies of this document from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

The DIGITAL logo is a trademark of Digital Equipment Corporation.

CONTENTS

1 INTRODUCTION 1
1.1 PURPOSE 1
1.2 SCOPE 1

2 GUIDELINES FOR DEVELOPING A PRODUCT FAULT MANAGEMENT SPECIFICATION 1
2.1 OVERVIEW 1
2.2 PROCESS 1
2.3 GENERATING AND USING THE PRODUCT FAULT MANAGEMENT SPECIFICATION 2
2.4 SCHEDULE OF ACTIVITIES 4
2.4.1 Pre-Phase 0 and Phase 0 Activities—Strategy and Requirements 6
2.4.2 Phase 1 Activities—Planning and Preliminary Design 6
2.4.3 Phase 2 Activities—Implementation and Design 7
2.4.4 Phase 3 Activities—Qualifications 8
2.4.5 Phase 4 Activities—Ramp Up and Steady State Operations 9

Appendix A REFERENCED DOCUMENTS 11
A.1 EL-Class Digital Documents 11

FIGURES

1 Product Fault Management Specification Building Blocks 3
2 Phase Activities 5

1 INTRODUCTION

This section of the standard provides a set of life cycle guidelines for developing a Product Fault Management Specification (PFMS). These PFMS life cycle guidelines adhere to the phase review process, defined in *DEC STD 028-0 Phase Review Policy*.

1.1 PURPOSE

The purpose of this standard is to provide detailed life cycle guidelines to developers of PFMS.

1.2 SCOPE

This section of the standard provides life cycle guidelines to developers of PFMSs. This section is not a standard.

2 GUIDELINES FOR DEVELOPING A PRODUCT FAULT MANAGEMENT SPECIFICATION

This segment of the standard provides life cycle guidelines for developing a PFMS and includes an overview, process, list of producers and customers, and phase number and activities.

2.1 OVERVIEW

A PFMS should be written in a manner that meets the requirements of the product team and end users of the specification. Information needed to support the field should also be described in a PFMS so that a standard reference document is available when creating service training courses, field documentation, and trouble-shooting procedures.

A PFMS contains information that can be used for the following:

- Understanding the product fault management strategy
- Defining and testing of error-detection mechanisms
- Defining and designing error handling during product development
- Testing of error handling during debug and verification
- Writing fault-handling algorithms for software fault management tools
- Creating fault-handling trouble-shooting and repair procedures
- Testing of fault handling during debug and verification

2.2 PROCESS

The evolution of a PFMS follows the corporate phase review process in parallel with the development of the product, including any pre-Phase 0 activity. A PFMS documents how the fault management strategy will be implementation and provides the detailed supporting information for the appropriate end users at the appropriate time. For example, in Phases 0, 1, and 2, a PFMS conveys error-handling and fault-handling information to the service tool, diagnostic, technical documentation and training course development groups. A PFMS serves as a trouble-shooting tool through Phase 4 and is updated to

reflect any subsequent fault management related engineering change orders (ECOs) and field change orders (FCOs) made to the product.

To track the development progress of a PFMS, milestones are defined and included in the engineering plans and the service plan. Figure 2 identifies the timing of the activities to be performed to meet the milestones.

Since the generation of a PFMS might start at a time other than during Phase 0, the document can be used to identify work to be done to catch up to the current phase. Even for those projects beyond Phase 3, procedures supplied in this document will allow the developer to reverse engineer a PFMS to create trouble-shooting rules for Digital Services.

Cases may exist where product development was begun before the start of the product's formal phase review process. The tool development schedule will require appropriate adjustment to catch up with the product's development schedule. It is the responsibility of the product team to ensure that the intent of the schedule is met.

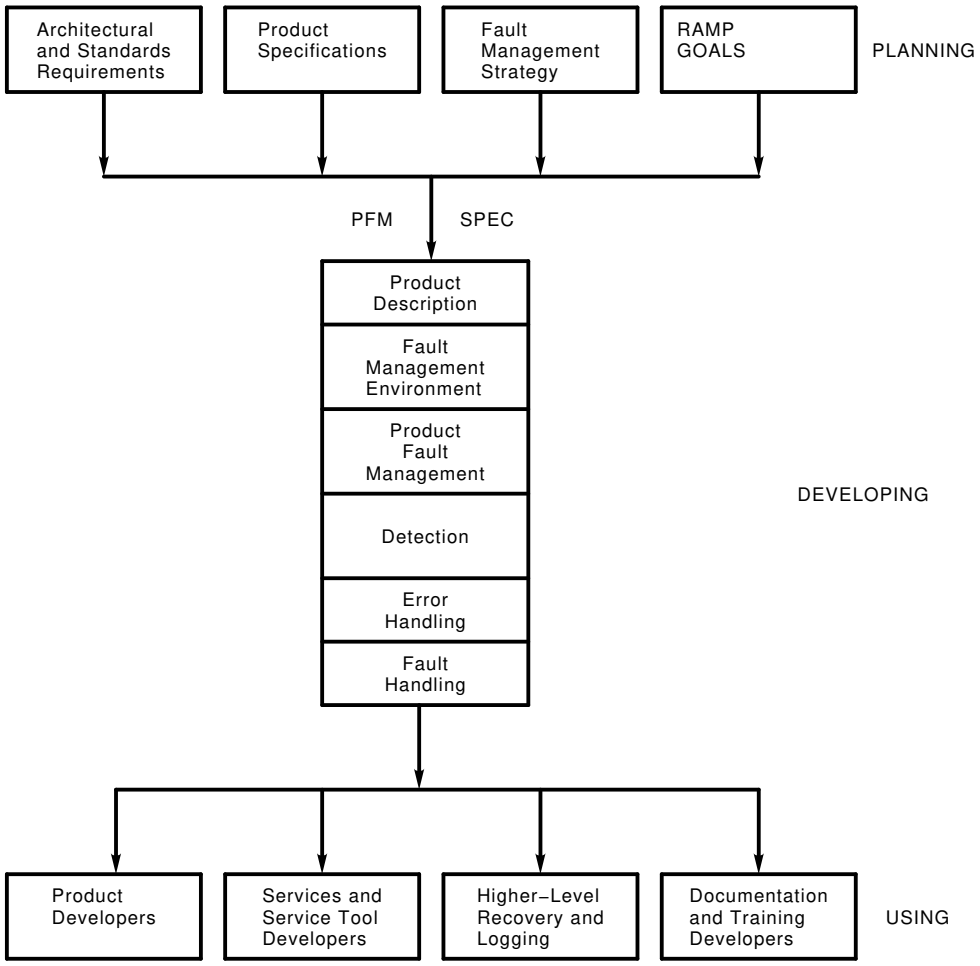
2.3 GENERATING AND USING THE PRODUCT FAULT MANAGEMENT SPECIFICATION

A PFMS is used to convey information to various groups at different times, depending on the phase of product development. The process of developing a PFMS involves research to understand the context of the product. The research is applied to the actual writing of a PFMS. The evolution of this specification is defined by the following sequence, and is illustrated in Figure 1.

Planning:

1. Study the architecture, standards, product requirements, product specifications, serviceability goals, and understand both the product and service marketplace.
2. Adopt a system level fault management strategy that meets the requirements listed in item 1.
3. Develop product-specific error-handling and fault-handling strategies that map into fault management strategy and support the achievement of both the system and product serviceability goals.

Figure 1: Product Fault Management Specification Building Blocks



Developing:

1. Write a PFMS based on the planning items listed previously in this section
2. Describe the product and the serviceability goals
3. Document how the fault management strategy will be implemented
4. Define and document the placement of error-detection mechanisms in the product
5. Document the reporting mechanisms
6. Define the error-recovery procedures
7. Define the format and contents of the event reports at each interface
8. Provide a translation of the information contained in the event reports
9. Define the fault-isolation procedures

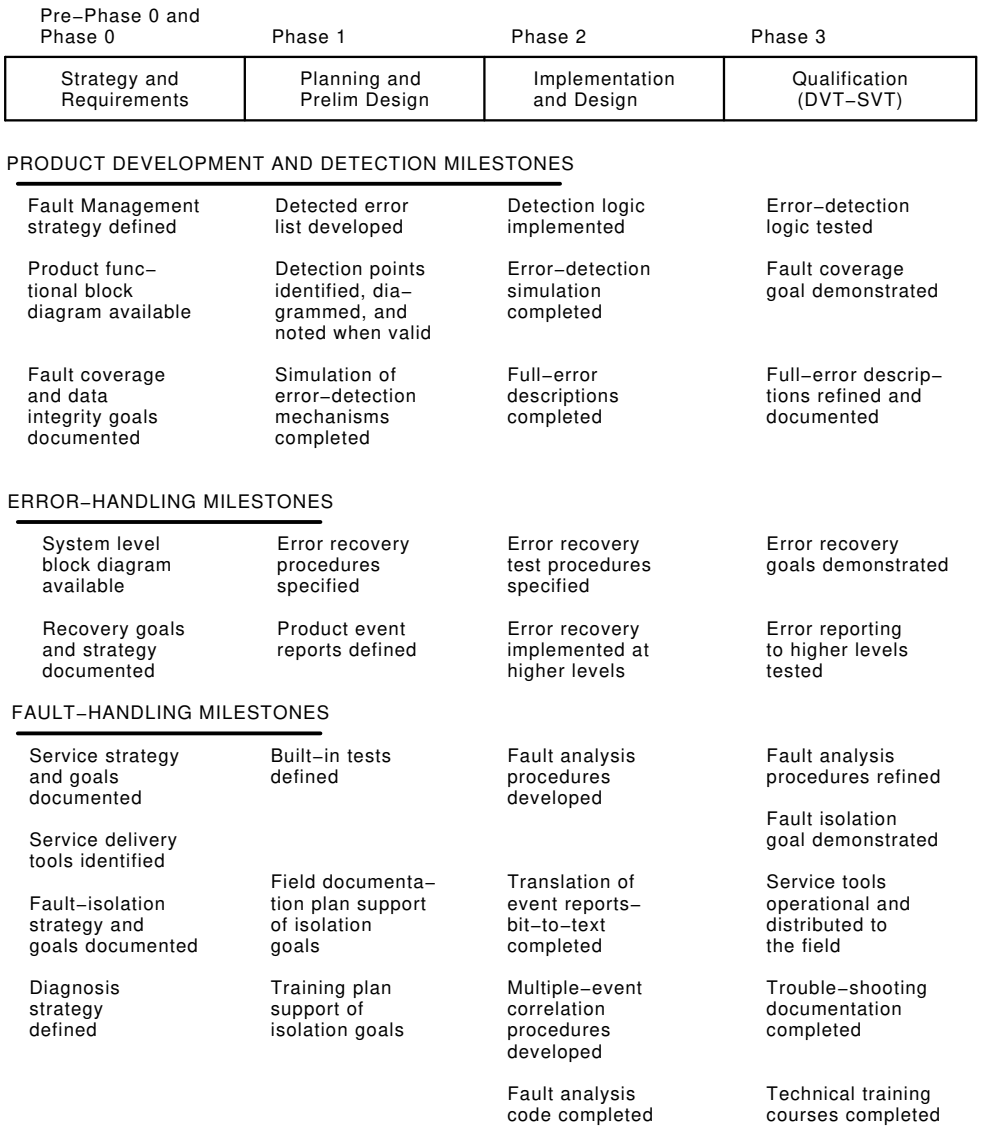
Using:

1. Create the service fault management tools
2. Develop the higher-level error recovery
3. Develop the product's field diagnostics, documentation, and training
4. Develop the design verification test (DVT) and system verification test (SVT)

2.4 SCHEDULE OF ACTIVITIES

Figure 2 defines the timing of those activities necessary to produce a PFMS. A PFMS is maintained throughout the life cycle of the product, including ECO and FCO Phase 4 activities.

Figure 2: Phase Activities


Pre–Phase 0 and Phase 0
Phase 1
Phase 2
Phase 3
Strategy and Requirements
Planning and Prelim Design
Implementation and Design
Qualification (DVT–SVT)
PRODUCT DEVELOPMENT AND DETECTION MILESTONES
Fault Management strategy defined
Detected error list developed
Detection logic implemented
Error–detection logic tested
Product func–tional block diagram available
Detection points identified, dia–grammed, and noted when valid
Error–detection simulation completed
Fault coverage goal demonstrated
Fault coverage and data integrity goals documented
Simulation of error–detection mechanisms completed
Full–error descriptions completed
Full–error descrip–tions refined and documented
ERROR–HANDLING MILESTONES
System level block diagram available
Error recovery procedures specified
Error recovery test procedures specified
Error recovery goals demonstrated
Recovery goals and strategy documented
Product event reports defined
Error recovery implemented at higher levels
Error reporting to higher levels tested
FAULT–HANDLING MILESTONES
Service strategy and goals documented
Built–in tests defined
Fault analysis procedures developed
Fault analysis procedures refined
Service delivery tools identified
Fault isolation goal demonstrated
Field documenta–tion plan support of isolation goals
Translation of event reports–bit–to–text completed
Service tools operational and distributed to the field
Fault–isolation strategy and goals documented
Diagnosis strategy defined
Training plan support of isolation goals
Multiple–event correlation procedures developed
Trouble–shooting documentation completed
Fault analysis code completed
Technical training courses completed

2.4.1 Pre-Phase 0 and Phase 0 Activities—Strategy and Requirements

During pre-Phase 0 and Phase 0, the product strategy and requirements are defined in the product requirements document. Engineering defines the major components for the product, including the interfaces and structures between them.

Engineering and Digital Service define the product requirements needed to support the achievement of the data integrity and service goals. The following list describes the major activities that are performed:

- Gain understanding of the architecture and product requirements.
- The product Reliability, Availability, and Maintainability Program (RAMP) goals are defined. For example, fault coverage, error recovery, fault isolation, availability, and data integrity goals.
- The product fault management implementation strategy is documented.
- A product functional block diagram is developed which becomes the frame of reference for the product team members.
- The service delivery tools that will support the product are identified.

At the end of Phase 0, the following fault management information should be available:

- The level of fault coverage and type of detection mechanism should be agreed upon by serviceability engineering and engineering. This agreement should be documented in the engineering design specification.
- A product definition and a fault management implementation strategy should be documented.
- A description of the service tools necessary to provide support for the product is agreed upon.
- A functional block diagram is in place.
- A system-level block diagram that includes the product configuration is in place.

2.4.2 Phase 1 Activities—Planning and Preliminary Design

In Phase 1, product planning occurs and engineering develops the product *functional specification*. The PFMS is developed in parallel with the functional specification. The following activities are performed during Phase 1:

- Document the location of those detection mechanisms that were used to achieve the fault coverage, isolation, and data integrity goals of the product. Determinimg the fault coverage is accomplished by understanding the architecture requirements for the product, the *Design Specification* for the product, the product strengths and weaknesses. Based on this understanding, detection points and detection mechanisms are defined to fulfill those requirements.
- One or more block diagrams with detection points are included and shall become the frame of reference for error detection and error handling for the product.
- Error detection points are defined in such a way that the fault coverage for the product meets the RAMP goals. The fault coverage goals defined in Phase 0 become the basis for the planned placement of error detectors.

- Simulation techniques are used to evaluate the effectiveness of different types of error detection mechanisms and the effectiveness of their placement.
- A *list of detection points* is created based on the detectors. The list shall consist of an error definition and an error name that is consistent with similar products so the meaning is consistent across products, for example, *NAME: Data Memory Parity Error*, and *DEFINITION: Some words that describe what Data Memory Parity Error means*.

  In the ideal situation, the list of detection points should be complete when design engineering is ready to start schematic capture or to start prototype coding. The design is in such a state of flux that having a complete list is not always realistic. It is imperative that a list of detection points exists that represents the latest design as closely as possible.

  At this time, the list of detection points is not in concrete, but is simply a list of required error-detection mechanisms and associated context that design engineering should incorporate into the product. As the design develops, error-detection mechanisms may need to be added to the design and some that were already agreed upon may have to be moved or removed. Whichever the case, design engineering and serviceability engineering should agree to the change that should then be included in the PFMS, and the change documented in the revision section maintained in an appendix of the PFMS.
- Error-handling and recovery procedures are defined for each detected error. The procedures should be divided into classes or types based on architecture definition, similar products, or similar reporting and signaling mechanisms internal to the product.
- Higher-level error-handling requirements are defined, if required.
- Fault analysis information should reflect the current understanding of the design.

At the end of Phase 1, the following fault management information should be available:

- For each detectable error, an error description should be written and should reflect the current understanding of the error.
- The content of the error description for each currently agreed-upon detectable error should include the error description, error code, detection point, related state, recovery procedure, and reporting mechanisms.
- An up-to-date product functional block diagram including detection points should now be available.

2.4.3 Phase 2 Activities—Implementation and Design

The product is built during Phase 2. The PFMS should now be complete enough to serve as the guideline for implementing error handling. During implementation, any changes that occur that affect error handling shall be reviewed against the PFMS to ensure that serviceability and data integrity are not jeopardized. Changes to error handling shall be documented in the PFMS and the changes noted in the revision section of an appendix of the PFMS.

This phase of the design starts at the schematic capture and proceeds through prototype. This phase of product development is where *all* agreed-upon error-detection mechanisms in the list of detection points are implemented into the design. During this phase, the design engineers work to refine the environment, detection point, reporting and signaling, and recovery or retry associated with each error. When the prototype phase has completed, *all* error detection mechanisms and associated context required for fault isolation should be designed into the product, as defined in the list of detection points. Again, this is not to say that all error-detection mechanisms are cast in concrete; but through the prototype phase, some context information might change even the lists of detection points. Any changes shall be documented in the PFMS.

Design activitites and actions for Phase 2 include:

- Completing the error descriptions
- Defining the test procedure for each detected error
- Completing the fault analysis for each detected error
- Completing bit to text translation of event report information
- Writing fault analysis code based on the fault analysis information
- Developing multiple-event correlation theories
- Developing error-handling and fault-handling test procedures

Additional dependencies required to complete the tasks include the following:

- A simulation to test and evaluate the fault manager
- A simple set of event report packets to test the algorithms implemented in the higher-level fault managers
- A mechanism to emulate the protocol between the product and fault manager

2.4.4 Phase 3 Activities—Qualifications

During Phase 3, DVT and SVT are performed to qualify the product. A qualification team performs the SVT of the product and the DVT of the fault management functions. The information in the PFMS is used to document the simulated or manually inserted fault points that will be used to ensure that detection mechanisms provide adequate coverage of faults.

Phase 3 activities include the following:

- Information from the PFMS is used to define the system's error-handling test procedures. The implementation of these test procedures is the basis for proving that the system handles errors as specified.
- Results of handling each error along with all related fault-handling information is captured in the event report as specified by the PFMS. The event report is sent to a sink where it will be placed in an event and error log. The test procedures for verifying the reporting and logging of information according to the PFMS are implemented.
- The fault management process is tested to verify that detected errors are managed properly.
- Error log messages or event reports are provided to test the fault-isolation algorithms.

- Documentation developers should use the information in the PFMS to support the development of the following documentation:
  - — The error-handling information in the service manual based on documented error descriptions
  - — Trouble-shooting procedure information in the service manual using the fault-isolation procedures and error descriptions.
  - — FRU isolation information in the maintenance guide and service manual using the fault-isolation data of the error description.
  - — The fault management environment and error description information shall be included in the technical description manual.

2.4.5 Phase 4 Activities—Ramp Up and Steady State Operations

During Phase 4 the PFMS is maintained. The PFMS is used in the ECO and FCO processes and updated to reflect any changes made in the area of fault management. It can be used to support trouble-shooting in the field.

APPENDIX A REFERENCED DOCUMENTS

A.1 EL-Class Digital Documents

EL-Class Number	Document Title
EL-00028-00	*DEC STD 028-0 Phase Review Policy*

Use VTX SMC to order copies of EL-class documents from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

```
+-------------------------------------------------------------------+
|                        READER COMMENTS                            |
|                                                                   |
| Your  comments  and suggestions  will help  Standards and Methods |
| Control improve their services and documents.                     |
+-------------------------------------------------------------------+
```

Did you request this document? _____ If so, did it arrive within a satisfactory period of time? _____ Please comment.

What are your impressions of this document? Consider format, organization, completeness, readability, and illustrations.

————————**FOLD ON THIS LINE**———————————————— -

Did you find technical or clerical errors in this document? If so, please specify the page number(s) and the error(s).

Are the instructions for the update package clear? _____
Was an index available? _____ If not, is one needed? _____
Do you have other suggestions for improving this document?

The following information is optional:

Name _____ Mailstop _____

Department _____ Node _____

Send your comments to JOKUR::PROJECTS, or fold, staple, and send this page through interoffice mail to:

```
+------------------------------+
|       READERS' COMMENTS      |
| STANDARDS AND METHODS CONTROL |
|           NRO4/D4            |
+------------------------------+
```